AO 106 (Rev. 04/10) Application for a Search Warrant

JH 10/25/2019

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The residence located at 3252 Yellow Finch Way, Columbus, Ohio 43231, including any curtilage and any computers, cellular phones and/or other electronic devices located therein

Case No. 19mj 848

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A1 INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

FILED
RICHARD W. NAGEL
CLERK OF COURT
2019 OCT 25 PM 1:56
U.S. DISTRICT COURT
SOUTHERN DISTRICT OHIO
EAST. DIV. COLUMBUS

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Secs 1028, 1028A, 1030, 1343, 1344, 1349, 371, 1956, and 1957	Identity theft, Aggravated identity theft, Computer hacking, Wire fraud, Bank fraud, Conspiracy to commit wire/bank fraud, Conspiracy, Money laundering/conspiracy to engage in money laundering, and transactions in criminally derived property

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Seth Erlinger, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10-25-19 1:48

Judge's signature

City and state: Columbus, Ohio

CHELSEY M. VASCURA, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, SETH ERLINGER, having been duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants authorizing searches of the following location and person for the things described in Attachment B:

   a. 3252 Yellow Finch Way, Columbus, Ohio 43231 (located within the incorporated district of Minerva Park), as further described in Attachment A1 ("Subject Location"); and

   b. Suleman Wadur, a.k.a. Suleman Bulama Wadur ("Wadur"), as further described in Attachment A2, including any wireless telephone he possesses, owns, maintains, or operates.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since September 2017. I am currently assigned to the Cincinnati Field Office, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes, and I am trained and authorized to investigate the offenses alleged herein. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations.

3. The facts and information contained in this affidavit are based on, among other things, my knowledge and observations, my training and experience, a review of evidence, and information from witnesses and other law enforcement personnel.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. Unless otherwise noted, I describe communications in summary and in part and, where I set forth dates, figures, times, and calculations, they are approximate.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to search the location described in Attachment A1 and the person described in Attachment A2 for evidence and instrumentalities of violations of federal law, including 18 U.S.C.

§§ 1028 (identify theft), 1028A (aggravated identity theft), 1030 (computer hacking), 1343 (wire fraud), 1344 (bank fraud), 1349 (conspiracy to commit wire and bank fraud), 371 (conspiracy), 1956 (money laundering and conspiracy to engage in money laundering), and 1957 (transactions in criminally derived property) (collectively, "subject offenses").

6. The applied for warrants would authorize the forensic examination of any electronic devices seized pursuant to the warrants to identify electronically stored data particularly described in Attachment B.

II. PROBABLE CAUSE

A. Summary

7. The Federal Bureau of Investigation ("FBI") and the Department of Defense, Defense Criminal Investigative Service ("DCIS") are investigating an ongoing business email compromise ("BEC") scheme and connected romance scheme through which the subjects of the investigation fraudulently obtained and attempted to obtain millions of dollars from companies and individual victims. The investigation also has revealed that subjects in the United States are laundering the funds obtained through the schemes, at the direction of others, many of whom law enforcement believe are located in Nigeria. Subjects living in the United States include Wadur, Michael Oghale Uziewe, a.k.a. Michael Uziewe Oghale (Uziewe), and Omodotun Titus Durojaye, a.k.a Titus Omodotun Durojaye ("Durojaye").

8. The majority of funds fraudulently obtained initially have been deposited in accounts in the names of purported entities, including Global Investment Network Inc. ("Global Investment"), Hasmaya Group LLC, f.k.a. Hasmaya Energy Group Ltd. ("Hasmaya"), and Deuteronomy Procurement Services, LLC ("Deuteronomy"). After funds are deposited in entity accounts, they generally are disbursed to accounts in other entities' and individuals' names through wire transfers and cashier's checks. Substantial amounts of funds also are withdrawn in cash. Funds law enforcement have been able to trace generally are sent to accounts overseas, including accounts in Nigeria. Additionally, fraudulently-obtained funds are used to purchase and ship vehicles overseas, including to Nigeria.

9. Through the investigation, I and other law enforcement agents determined: (a) Uziewe controls financial accounts in Global Investment's name, among others; (b) Durojaye controls financial accounts in Deuteronomy's name, among others; and (c) Wadur controls financial accounts in

Hasmaya's name, among others. Uziewe, Durojaye, and Wadur all are Nigerian nationals currently living in the United States. Wadur lives at the Subject Location.

10. I and other law enforcement agents also have identified an individual we believe is one of the leaders of the scheme. Specifically, electronic communications related to the scheme refer to an individual named Evans Itedjere as the "chairman" and "boss." Internet Protocol addresses associated with electronic communications, as well as financial records, indicate that Itedjere and other subjects are located in Nigeria.

B. Background on Nigerian BEC and Romance Schemes

11. Based on the above, my training and experience, evidence obtained during the course of this investigation, and consultations with other law enforcement personnel, including a detective with the Nigerian Economic and Financial Crimes Commission ("EFCC"), I believe individuals located in Nigeria and their United States-based associates are directing and carrying out the BEC scheme, the connected romance scheme, and the laundering of funds obtained through the schemes. I also know the following:

12. BEC schemes often involve a computer hacker gaining unauthorized access to a business email account, blocking or redirecting communications to and from the email account, and then using the compromised email account or a separate, fraudulent email account to communicate with personnel from a victim company. The fraudulent actors attempt to trick victim company personnel into making unauthorized wire transfers to fraudulent accounts. One way in which fraudsters attempt to trick personnel is to create a domain name that appears identical to the businesses genuine account. For example, the fraudster will change one letter or add one letter to the genuine domain. The fraudster often will direct the unsuspecting personnel of the victim company to wire funds to the bank account of a third party (sometimes referred to as a "money mule"), which often is an account owned, controlled, or used by United States-based conspirators. Additionally, the fraudsters may direct victim company personnel to wire or otherwise move funds to a bank account of an unwitting third party who then transfers the money to an account controlled by a United States-based conspirator.

13. Romance schemes often are related to BEC schemes. The schemes generally take advantage of persons looking for romantic partners by targeting victims on dating websites and other

social media platforms. The fraud schemes often target victims who are elderly or otherwise vulnerable to online schemes. The scammers create profiles using fictitious or fake names, locations, images, and personas, which they use to cultivate relationships with victims. And the scammers use electronic communications, such as text messages, third party messaging applications, online dating websites, forums, chatrooms, and email, to initiate a relationship with the targeted individuals. The scammers often use elaborate cover stories to convince victims to send money to designated financial accounts. One common ploy is to create a story that the romance scam actor is a member of the U.S. military deployed overseas who needs funds in order to return to the United States, so that they can continue their romantic relationship. Scammers also convince victims to conduct transactions on their behalves that they claim they cannot conduct from their overseas locations. They may do this by convincing a victim to transfer money deposited in the victim's bank account—often from another scam such as a BEC scheme—to an account the scammer or a conspirator controls. Romance scheme victims may thus become unwitting money mules for other fraudulent schemes when scammers direct them to transfer money through their bank accounts.

14. Funds obtained through BEC and romance scams often are deposited in accounts controlled by United States-based conspirators who then launder the funds and transfer them to conspirators overseas. The conspirators launder the funds in multiple ways, including by wiring or transferring them through numerous bank accounts, quickly withdrawing funds as cash, check, or cashier's check, and using funds to purchase vehicles sent overseas. After quickly draining victim funds from fraudulent accounts they create, United States-based conspirators often close the accounts.

C. Subjects and Related Entities

1. Uziewe – Global Investment Network Inc., Didimiki Global Enterprises Corporation

15. Uziewe is a Nigerian citizen who formerly lived in Nigeria. He now lives at the 1885 Pinehurst View Drive, Grayson, Georgia.

16. Uziewe's most recent driver license, which expires in 2024, lists his address as 1885 Pinehurst View Drive, Grayson, Georgia.

17. Uziewe controls multiple bank accounts under several names, including Global Investment, Didimiki Global Enterprises ("Didimiki"), and Michael Uziewe. 1885 Pinehurst View Drive, Grayson, Georgia, is the address associated with the following Uziewe-controlled accounts:

a. Global Investment

1) Bank of America, ending 4817
2) Bank of America, ending 0272
3) Brand Banking and Trust, ending 6925
4) JP Morgan Chase, ending 6302
5) SunTrust Bank, ending 3667
6) United Community Bank, ending 9218

b. Michael Uziewe

1) First IC Bank, ending 0839
2) SunTrust Bank, ending 3339
3) Wells Fargo, ending 0535

18. According to the most recent filing with the Georgia Secretary of State—an annual registration dated February 26, 2019—Global Investment is a domestic, for-profit corporation located at 1911 Grayson Highway, Suite 8-339, Grayson, Georgia. The filing lists Uziewe as the CEO, CFO, and Secretary. The filing also lists Uziewe as the registered agent, with 1885 Pinehurst View Drive, Grayson, Georgia, as his address. The original articles of incorporation list 1885 Pinehurst View Drive, Grayson, Georgia, as Global Investment's principal office address.

19. According to the most recent filing with the Georgia Secretary of State—an annual registration dated February 26, 2019—Didimiki is a domestic, for-profit corporation located at 1911 Grayson Highway, Suite 8-339, Grayson, Georgia. The filing list Uziewe as the CEO, CFO, and Secretary. The filing also lists Uziewe as the registered agent, with the Grayson Highway address as his address. The original articles of incorporation list 1885 Pinehurst View Drive, Grayson, Georgia, as the incorporator's address. The articles list Uziewe as the incorporator.

20. United Parcel Service ("UPS") records show that 1911 Grayson Highway, Grayson, Georgia, is the address of a UPS Store. And 339 is the number of a mailbox Uziewe rents in Global Investment's name at the store. In his application for the mailbox, Uziewe listed 1885 Pinehurst View Drive, Grayson, Georgia, as Global Investment's business address, as well as his home address.

21. Uziewe uses the Grayson UPS box address for multiple bank accounts he controls, including the following:

a. Global Investment

1) First IC Bank, ending 1180

2) South State Bank, ending 6302

3) Synovus Bank, ending 3410

b. Didimiki

1) Entegra Bank, ending 2175

2) SunTrust Bank, ending 4026

22. I and other agents were unable to locate a current, purported business address or physical location for either Global Investment or Didimiki, other than Uziewe's home address and the UPS box address. Based on that, my training and experience, and the investigation to date, I submit that Uziewe operates Global Investment and Didimiki from Uziewe's home address.

2. Durojaye – Deuteronomy Procurement Services, LLC

23. Durojaye is a Nigerian national and naturalized United States citizen who lives at the 8806 Purdy Crescent Trail, Richmond, Texas.

24. Durojaye's most recent driver license, which expires in 2022, lists his address as 8806 Purdy Crescent Trail, Richmond, Texas.

25. Durojaye controls multiple bank accounts under several names, including Deuteronomy, Eds Lead LLC, his name, including variations, and the name of his wife, Olabimbe Durojaye. 8806 Purdy Crescent Trail, Richmond, Texas, is the address associated with the following Durojaye-controlled accounts:

a. Deuteronomy

1) Bank of America, ending 3024

2) Wells Fargo, ending 5415

b. Durojaye individually and Durojaye and Olabimpe Durojaye jointly

1) Bank of America, ending 7433

2) Bank of America, ending 0769

3) Bank of America, ending 6444

4) Bank of America, ending 0261

5) Bank of America, ending 0167

26. Additionally, the following Durojaye-controlled accounts are associated with Durojaye's former residential address—3901 Abernathy Farm Way, Acworth, Georgia:

a. Eds Lead LLC

1) Wells Fargo Account, ending 0153

b. Durojaye and Olabimpe Durojaye jointly

1) Wells Fargo, ending 9865

2) Wells Fargo, ending 7962

3) Wells Fargo, ending 9812

27. According to a registration filed on January 16, 2019, with the Texas Secretary of State's Office, Deuteronomy is domestic limited liability company. The registered agent and owner is Durojaye, and the principal office address is 8806 Purdy Crescent Trail, Richmond, Texas.

28. According to the Texas State Comptroller's Office Franchise Tax Public Information Report for the 2018 reported year, Durojaye owns Deuteronomy, and 8806 Purdy Crescent Trail, Richmond, Texas, is Deuteronomy's mailing address.

29. I and other agents were unable to locate a purported business address or physical location for Deuteronomy, other than Durojaye's home address on Purdy Crescent Trail. Based on that, my training and experience, and the investigation to date, I submit that Durojaye operates Deuteronomy from his home.

3. Wadur – Hasmaya

30. Wadur is a Nigerian citizen who lives at the Subject Location.

31. Wadur's most recent driver's license, which expires in April 2021, lists his address as the

Subject Location.

32. According to the United States Postal Inspection Service, Wadur's previous residential address was 3124 Old Providence Lane, Westerville, Ohio. On October 23, 2018, Wadur filed a form to change his address to the Subject Location.

33. The following are Wadur-controlled accounts associated with Wadur's previous residential address—3124 Old Providence Lane, Westerville, Ohio:

a. Hasmaya

1) JP Morgan Chase, ending 6966

2) Keybank, ending 8802

3) PNC Bank, ending 6556

b. Wadur

1) JP Morgan Chase, ending 8917

34. The following are Wadur-controlled accounts using a purported business address for Hasmaya—470 Olde Worthington Road, Suite 200, Westerville, Ohio:

a. Hasmaya

1) Keybank, ending 8836

35. According to the original Articles of Organization filed with the Ohio Secretary of State's Office on August 11, 2014, Hasmaya was organized as a domestic for-profit Limited Liability Company with Wadur as its statutory agent. An amendment to the original filing, dated September 21, 2017, changed the name from Hasmaya Energy Group, LLC, to Hasmaya Group, LLC (dropping the Energy moniker), and listed Wadur as the statutory agent. A public records database indicates that Hasmaya's purported business address is 470 Olde Worthington Road, Suite 200, Westerville, Ohio.

36. Based on the investigation, I know Hasmaya's purported business address on Olde Worthington Road was a virtual office with no physical space. A federal agent spoke with a representative of the company from which Wadur rented the virtual office. The representative explained that Wadur's virtual office was not a physical office. Rather, Wadur used the address of the physical building, or "suite" in the building, to receive mail for Hasmaya. The representative said that, as of March 31, 2018, Wadur no longer had the virtual office. So, like Uziewe's use of the UPS box in

Grayson, Georgia, Wadur used the Olde Worthington Road address simply to receive mail.

37. I and other agents were unable to locate a purported business address or physical location for Hasmaya, other than the virtual office mailing address and Wadur's former home address. Based on that, my training and experience, and the investigation to date, I submit that Wadur operates Hasmaya from the Subject Location. I also submit that records related to Hasmaya, including financial and business records, are located at the Subject Location.

38. Public records database research revealed that Wadur is married to Bilkisu Aliyu Wadur. As of 2019, her current residence is the Subject Location. Additionally, the Ohio Department of Motor Vehicles identified Bilkisu Aliyu Wadur's current residence as the Subject Location. The Subject Location also is listed on her current driver license, which expires in February 2021.

39. On September 26, 2019, DCIS Special Agents conducted surveillance at the Subject Location and observed two vehicles registered to Wadur and his wife. In addition, the Franklin County Assessor confirmed Wadur and his wife purchased the Subject Location in November 2018.

40. Between September 25, 2019 and October 11, 2019, DCIS Agents surveilled the Subject Location ten times. During surveillance, Agents observed a white Mercedes C Class sedan and Grey Honda Accord Sedan. Ohio DMV records indicate Wadur owns the white 2006 Mercedes C Class sedan (License Plate GOJ8875) and the grey Honda Accord (License Plate HJM4921).

D. Scheme Victims

1. Victim Company 1 – BEC Scheme

41. Victim Company 1 is a cleared Department of Defense contractor headquartered in El Dorado Hills, California. The subject(s) of the investigation carried out the BEC scheme by posing as Victim Company 1 employees and convincing Victim Company 1 customers to send payments meant for Victim Company 1 to bank accounts not associated with Victim Company 1.

42. The subject(s) of the investigation perpetrated the scheme by, among other things, purporting to be Victim Company 1 employees such as the accounts receivable manager and sending emails from addresses that contained a domain name slightly different from Victim Company 1's authentic domain. Specifically, the fraudulent email account contained an additional letter in the domain name.

43. In email communications occurring between June 2017 and September 2017, the subject(s) falsely told Victim Company 1 customers that Victim Company 1 was updating its payment methods and provided wiring instructions for bank accounts not associated with Victim Company 1.

44. Between July 2017 and August 2017, one Victim Company 1 customer wired a total of approximately $537,050 in four separate wire transfers to a fraudulent bank account owned by P.P., a 60 year old woman from Denver, Colorado.

2. P.P. Romance Scam – Global Investment, Deuteronomy, and Hasmaya

45. In September 2018, federal agents interviewed P.P. During the interview, P.P. admitted she owned the bank account that received the approximately $537,050 in funds intended for Victim Company 1. P.P. said that, in January 2017, she met an individual purportedly named David Willson through an online dating website. P.P. communicated with Willson by email at willsond1959@gmail.com and through voice and text communications using a messaging application called Viber. Through email and Viber, Willson instructed P.P. to open the account, which she did on June 30, 2017, and receive funds Willson claimed he was using to pay debts. At Willson's direction, P.P. withdrew the money the Victim Company 1 customer wired to her account through cashier's checks made payable to Global Investment, Deuteronomy, and Hasmaya. P.P. believed she deposited the cashier's checks into the destination accounts.

46. Financial records show the following:

a. Uziewe

47. P.P. purchased an approximately $24,000 cashier's check payable to Global Investment. On July 24, 2017, the check was deposited in an Uziewe-controlled JP Morgan Chase account ending in 6302. Uziewe opened the account on June 13, 2017, in Global Investment's name, and closed it on September 7, 2017.

48. On July 25, 2017, Uziewe wrote two checks totaling approximately $30,000 from the account to himself.

b. Wadur

49. P.P. purchased an approximately $302,290 cashier's check payable to Hasmaya. On July 24, 2017, the check was deposited in a Wadur-controlled PNC Bank account ending in 6556. Wadur

opened the account on June 8, 2017, in Hasmaya's name, and closed it on August 25, 2017.

50. Following the deposit of P.P.'s cashier's check, Wadur engaged the following transactions, among others, before closing the account:

a. Three cash withdrawals totaling approximately $27,225.

b. Three wire transfers totaling approximately $89,500 to a purported company called Dunkuul, Inc.

c. Issued seven cashier's checks totaling approximately $111,349 to Copart, an online auto auction site.

d. Issued an approximately $8,000 cashier's check to Insurance Auto Auctions, which was used as a partial payment for five vehicles purchased by H&H Honda MotoSpare Parts LTD located in Jani, Nigeria.

e. Two wire transfers totaling approximately $45,000 to two law firms located in Chicago, Illinois, and Baltimore, Maryland, respectively.

f. An approximately $25,000 wire transfer to a medical center in Florida.

g. An approximately $2,900 wire transfer to an individual named Babatunde Dowadu.

h. An approximately $2,500 wire transfer to an individual named Nura Muhtar.

c. Durojaye

51. P.P. purchased an approximately $204,845 cashier's check payable to Deuteronomy. On August 9, 2017, the check was deposited in a Durojaye-controlled Wells Fargo account ending in 5415. Durojaye opened the account on July 11, 2017, in Deuteronomy's name, and closed it on November 9, 2017.

52. Between August 9, 2017, and August 28, 2017, Durojaye initiated eight wire transfers totaling approximately $214,568 to a purported company called Deuteronomy Integrated Services. Durojaye sent the majority of the funds to accounts at First City Monument Bank in Lagos, Nigeria, by wire transfers through a Citibank intermediary account.

3. M.E. Romance Scam – Global Investment

53. In January 2019, federal agents interviewed M.E., a 75 year old woman from Evergreen, Alabama. During the interview, M.E. said she was involved in a romantic online relationship with an

individual who introduced himself as Vinskey Walker. M.E. first began communicating with Walker after her husband died in 2015. Walker claimed he was a "Lieutenant Commander" in the United States Army deployed to Iraq. Walker and M.E. initially communicated on Facebook Messenger, but at Walker's direction, the communications switched to the Google Hangouts application associated with Walker's Google account—westpointus2207@gmail.com—and M.E.'s personal Google account.

54. Around July 2018, Walker convinced M.E. to issue Global Investment a check for $55,649, which came from her own funds. Walker claimed the funds were to obtain his goods and retrieve documents he needed to give the Pentagon so he could retire and return to the United States. On July 23, 2018, Uziewe cashed M.E.'s check at a company called Atlanta Check Cashers.

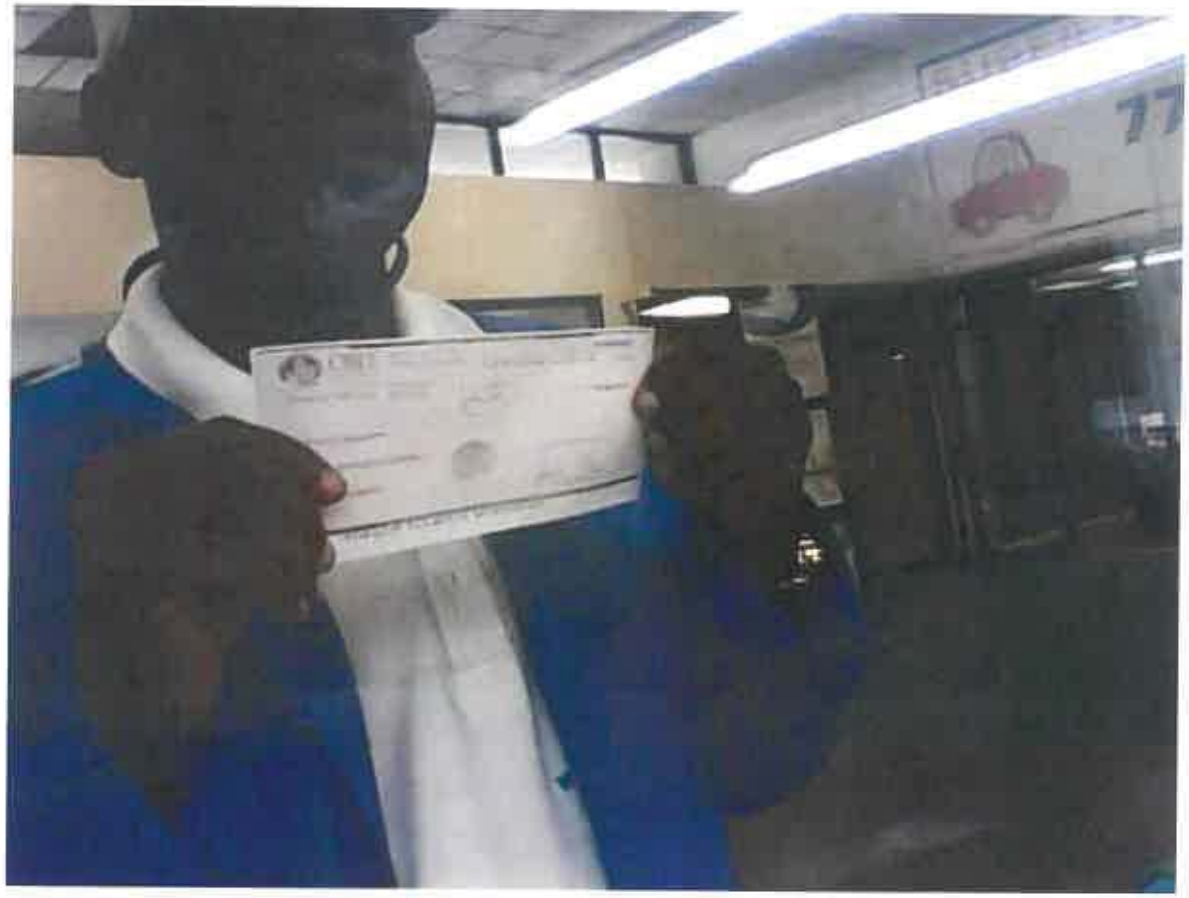
55. Around August 2018, Walker convinced M.E. to pay an additional $36,249 to Global Investment purportedly for costs associated with shipping Walker's goods. On August 30, 2018, Uziewe deposited an approximately $36,249 cashier's check from M.E., which he endorsed, in an Uziewe-controlled Synovus Bank account ending in 3410. Uziewe opened the account on August 6, 2018, in Global Investment's name, and closed it on November 30, 2018. After depositing the check, Uziewe wrote three checks to himself totaling approximately $36,500.

56. Subsequently, Walker attempted to convince M.E. to pay Global Investment an additional $169,000 or $187,000 to pay a tariff on Walker's goods, which purportedly were stopped at a port in Denmark. M.E. became doubtful about the situation and did not send any additional money.

4. C.C. Romance Scam – Global Investment

57. In March 2019, federal agents interviewed C.C., a 63 year old woman from Lacey, Washington. During the interview, C.C. said she was involved in a romantic online relationship with an individual who introduced himself as Nick Johnson. Johnson claimed he worked in the medical field and was stationed at "Joint Base Lewis McChord" in Washington. Shortly after their initial contact, Johnson told C.C. he was being deployed overseas. Johnson and C.C. initially communicated on Match.com, but at Johnson's direction, the communications switched to text and phone calls.

58. Around June 1, 2018, Johnson convinced C.C. to issue Global Investment a check for $60,000, which came from her own funds. On June 4, 2018, Uziewe cashed C.C.'s check at Atlanta Check Cashers. Below is a photograph of Uziewe doing so:



59. C.C. estimated she gave approximately $200,000 to Nick Johnson, during the course of their relationship.

5. P.B. Romance Scam – Global Investment and Others

60. In June 2019, federal agents interviewed P.B, a 77 year old woman from Greenville, South Carolina. During the interview, P.B. stated that, in November 2016, an individual purportedly named Eric George contacted her on Facebook. George claimed he was a "United States General" stationed in Baghdad, Iraq, and assigned to the "10th Mountain Division." P.B. assumed George was friends with a former friend of hers who was in the military. P.B. began communicating with George through Google Hangouts, a communication application, with George using the email address

westpoint1944@gmail.com.

61. In February 2018, George began asking P.B. for money. Between February 2018 and February 2019, P.B. issued multiple checks to various companies at the direction of people with whom George put her in contact—individuals purportedly named Steve Caurro and Matthew Reddington. Caurro claimed to be with "Source Diplomatic Services" and used email addresses source-diplomatic0101@outlook.com and source_deliveryunit@post.com to communicate with P.B. Reddington claimed to be with the United States Department of State's "B Divison" and used email addresses bdivision2207@yahoo.com and sourcecompany@europe.com to communicate with P.B.

62. In August 2018, Reddington directed P.B. to send an approximately $100,000 check to Global Investment. The purported purpose of the check was to facilitate getting George's personal belongings out of Baghdad and help him leave the army. On August 8, 2018, Uziewe deposited an approximately $100,000 cashier's check from P.B., which he endorsed, in an Uziewe-controlled Synovus Bank account ending in 3410. Uziewe opened the account on August 6, 2018, in Global Investment's name, and closed it on November 30, 2018. After depositing the check, among other transactions, Uziewe purchased a cashier's check for $93,000 that references a real estate purchase in the memo line, issued a personal check to himself for $4,900 that references office expenses in the memo line, and withdrew $15,000 in cash.

63. In addition to sending the $100,000 check to Global Investment, at Caurro's and Reddington's directions, P.B. issued multiple other checks to purported companies in New York City, New York, Atlanta, Georgia, and Lawrenceville, Georgia. Those checks totaled over $400,000.

6. K.P. Romance Scam – Global Investment

64. In June 2019, federal agents interviewed K.P., a 63 year old woman from Punta Gorda, Florida. During the interview, K.P. said someone purportedly named Mark Brenes Keller scammed her. K.P. said Keller contacted her in February of 2018 using Facebook Messenger. Keller claimed he was a General in the military stationed in Afghanistan. Keller said his wife passed away from breast cancer and he had a son named Jeff who was in military school. Keller sent K.P. several images that included purported photographs of him, his dead spouse, his son, and his dog. K.P. and Keller communicated frequently for approximately nine months using Facebook Messenger.

65. After initiating communications, Keller began asking K.P. for money. In total, Keller scammed K.P. out of approximately $291,200.

66. At Keller's direction, K.P. attempted to obtain a cashier's check from her account at a federal credit union. After speaking with K.P., however, a credit union employee believed K.P. potentially was being scammed and refused to issue the check. Subsequently, K.P. withdrew her funds from her credit union account and deposited them in a newly-opened account. At Keller's direction, in August 2018, K.P. obtained an approximately $205,000 cashier's check payable to Global Investment and sent it through the United States Postal Service to an address Keller provided. K.P. believed Global Investment was a realtor, as Keller said the $205,000 was to purchase a home for K.P. and Keller in South Carolina. On August 20, 2018, Uziewe deposited the $205,000 cashier's check from K.P., which he endorsed, in an Uziewe-controlled Synovus Bank account ending 3410—the same account into which Uziewe deposited P.B.'s $100,000 cashier's check. Following the deposit, Uziewe wrote five personal checks to himself totaling approximately $81,500, and an approximately $18,000 check that references advertising and promotion to an individual named Akpoho Otejiri. He also wired approximately $100,000 to a truck dealership in Mississippi.

67. In addition to obtaining and sending the cashier's check to Global Investment, K.P. also sent Keller approximately $2,950 purportedly to pay for Keller's son to take a trip related to his military school. K.P. also sent Keller approximately $75,000 purportedly to cover Keller's costs to return home from Afghanistan. Additionally, at Keller's direction, K.P. purchased approximately $5,000 in Apple iTunes gift cards and gave Keller the gift card codes.

68. After convincing K.P. to send money and gift card codes, Keller stopped communicating with her.

7. M.B.B. Romance Scam – Global Investment

69. In April 2019, federal agents interviewed M.B.B., a 67 year old woman from Cody, Wyoming. During the interview, M.B.B. said that, in approximately May 2018, she began communicating with an individual purportedly named Walter Ramsey Fernandes. M.B.B. communicated almost daily with Fernandes through Facebook, text messages, and telephone calls. Fernandes claimed he was an engineer working for NATO and had been on a ship over a year.

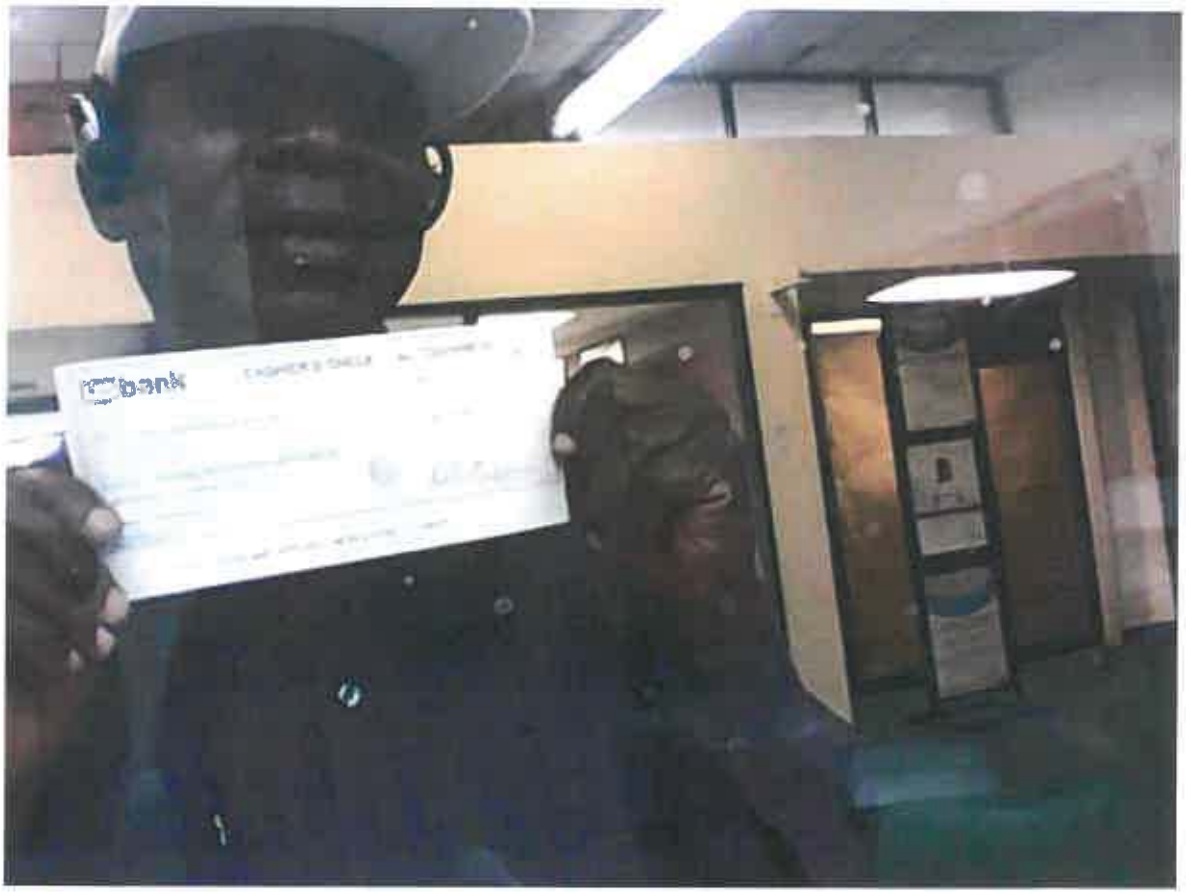
70. In June 2018, at Fernandes' request, M.B.B. began sending funds to various individuals and for varying reasons, including to pay for shipping packages to her, to pay Interpol and the FBI so they would not confiscate packages he sent, and to pay bribes to foreign officials.

71. Between June 2018 and March 2019, M.B.B. engaged in approximately ten transactions at Fernandes' request. The transactions totaled approximately $368,930 and included, among others, the following:

a. On July 30, 2018, M.B.B. sent an approximately $25,000 personal check payable to Global Investment to an address in Decatur, Georgia. On August 6, 2018, Uziewe deposited the check, which he endorsed, in the Synovus account ending in 3410 he controlled—the same account into which he deposited P.B.'s $100,000 cashier's check and K.P.'s $205,000 cashier's check.

b. On September 18, 2018, M.B.B. sent an approximately $39,000 personal check payable to Global Investment to 1911 Grayson Highway, Grayson, Georgia (i.e., the UPS store address Uziewe uses as the business address for Global Investment). On September 19, 2018, Uziewe deposited the check in the Synovus account.

72. Additionally, on July 12, 2018, M.B.B. sent an approximately $60,000 cashier's check payable to Global Investment to an unknown address. Subsequently, Uziewe cashed M.B.B.'s check at Atlanta Check Cashers. Below is a photograph of Uziewe doing so:



73. On September 28, 2018, after depositing and cashing M.B.B.'s funds, Uziewe wrote a $104,346 personal check to a purported company called Corner Global Medical Equipment Procurement LLC. He wrote the check from the Synovus account ending 3410. The check references the purchase of medical equipment.

8. K.J. Romance Scam – Hasmaya

74. In March 2019, federal agents interviewed K.J, a 62 year old woman from Melbourne, Florida. During the interview, K.J. said she was a widow and had met an individual on Match.com approximately three years ago. K.J. also confirmed she was defrauded of approximately $1,000,000. Of that $1,000,000, on June 13, 2017, she wired approximately $55,000 to a Wadur-controlled JP Morgan Chase account ending in 6966. Wadur opened the account on June 2, 2017, in Hasmaya's name, and closed it on August 14, 2017.

75. Wadur disbursed the majority of the $55,000 through transactions on June 14, 2017: he

transferred $3,600 from the JP Morgan Chase account to an unknown Bank of America account, and he purchased three cashier's checks totaling $51,550 payable to Copart, an online auto auction company.

E. Suspicious Accounts held by Uziewe, Durojaye, and Wadur

76. As noted above, United States-based conspirators involved in BEC and romance schemes launder victim funds in multiple ways. One way in which they do this is by opening fraudulent accounts to receive victim funds, quickly draining the accounts by cash withdrawals and checks to themselves and other fraudulent accounts, wire transfers to other fraudulent accounts or conspirators overseas, as well as purchases of vehicles they send overseas. Numerous accounts held by Uziewe, Durojaye, and Wadur, respectively, exhibit transactions indicative of this type of laundering. Law enforcement deemed the accounts discussed below as suspicious for multiple reasons, including, among others, (a) large deposits and cash withdrawals in quick succession, (b) wire transfer deposits from various, seemingly unrelated businesses and industries, (c) deposited checks from middle-aged and elderly women, (d) large international transfers to multiple countries such as Nigeria, China, and India, and (e) vehicle purchases.

1. Uziewe

77. Before January 1, 2015, a Wells Fargo Bank account ending in 7815 was opened in Global Investment's name. The account was closed on December 30, 2016. Between January 2, 2015, and December 30, 2016, there were a total of 398 credits to the account and 648 debits from the account. The credits totaled approximately $203,599, and the debits totaled approximately $204,052.

a. Significant credits include approximately $159,886 in cash and ATM deposits.

b. Significant debits include approximately $106,712 in cash and ATM withdrawals.

78. On October 30, 2015, Uziewe opened a SunTrust Bank account ending in 3339. He opened the account in his own name and closed it on June 27, 2017. Between October 30, 2015, and June 27, 2017, there were a total of 313 credits to the account and 376 debits from the account. The credits totaled approximately $412,011, and the debits totaled approximately $412,073.

a. Significant credits include approximately $369,072 in cash deposits.

b. Significant debits include:

i. Approximately $110,734 in cash withdrawals.

ii. Six wire transfers totaling approximately $110,520 to Ovuomarhoni Naomi Isioro

in Lagos, Nigeria.

iii. Four wire transfers totaling approximately $47,594 to Rowly Isioro in Nigeria.

iv. An approximately $8,000 wire transfer to a purported company called AOC Oasis Gases Nigeria LTD in Nigeria.

v. Four wire transfers totaling approximately $30,270 to various purported businesses in China called Great Decors Co, LTD, and Anshan N&M Foods Co, LTD, and to an individual named Ojewale Afeez.

79. On February 16, 2017, Uziewe opened a SunTrust Bank account ending in 3667. He opened the account in Global Investment's name and closed it on July 11, 2017. Between February 16, 2017, and July 11, 2017, there were a total of 160 credits to the account and 112 debits from the account. The credits and debits each totaled approximately $630,903.

a. Significant credits include:

i. Approximately $523,775 in cash deposits.

ii. The approximately $18,250 wire transfer from romance scam victim V.F. referenced above.

b. Significant debits include:

i. Eleven wire transfers totaling approximately $266,592 to Ovuomarhoni Naomi Isioro in Lagos, Nigeria.

ii. An approximately $44,800 wire transfer to Adefemi Adeniyi in Nigeria

iii. An approximately $25,500 wire transfer to Dominic Eloho Uziewe in Nigeria.

iv. Approximately $37,340 in cash withdrawals.

v. Fifty six checks totaling approximately $104,031 that Uziewe wrote himself.

vi. Approximately $65,300 in wire transfers to purported companies in China called Fuzhou Yiqun Handcraft Product LTD and HFX Co LTD and individuals named Ojewale Afeez and Gabriels Chikodi Christian.

80. On May 8, 2017, Uziewe opened a Bank of America account ending in 4817. He opened the account in Global Investment's name and closed it on August 18, 2017. Between May 8, 2017, and August 18, 2017, there were a total of 56 credits to the account and 48 debits from the account. The

credits and the debits each totaled approximately $334,155.

a. Significant credits include:

i. Cash deposits of approximately $125,098.

ii. An approximately $68,475 wire transfer from a private business in Cleveland, Ohio.

b. Significant debits include:

i. Thirteen cash withdrawals totaling approximately $121,812.

ii. Two wire transfers totaling approximately $65,178 to Ovuomarhoni Naomi Isioro in Lagos, Nigeria. Both transfers reference land purchases in Nigeria.

iii. An approximately $29,800 wire to a software company in Bulgaria that references a hardware and software purchase.

81. On June 13, 2017, Uziewe opened a JP Morgan Chase Bank account ending in 6302. He opened the account in Global Investment's name and closed it on September 7, 2017. Between June 13, 2017, and September 7, 2017, there were a total of 146 credits to the account and 186 debits from the account. The credits and debits each totaled approximately $1,457,099.

a. Significant credits include:

i. Approximately $304,368 in cash deposits.

ii. Approximately $552,108 from a variety of purported businesses, including remodeling, investment, technology, and vehicle businesses.

iii. The approximately $24,000 check from romance scam victim P.P. that was comprised of funds from the BEC scheme targeting Victim Company 1.

iv. Approximately $40,000 from MoneyGram.

b. Significant debits include:

i. Eight wire transfers totaling approximately $407,540 to Ovuomarhoni Naomi Isioro in Lagos, Nigeria, that reference business expenses, salary for building construction workers, building materials, auto show room construction expenses, land development, and a partial payment for a 5,000 square foot piece of land in Lagos, Nigeria.

ii. Twenty one separate checks totaling approximately $231,550 that Uziewe wrote to himself.

iii. Three wire transfers totaling approximately $162,500 to a company in Mumbai, India, that reference "34-unit point of sale," "105-unit point of sale," and "500-unit point of sale," respectively.

iv. Two wire transfers totaling approximately $71,955 to a company in Brussels, Belgium.

82. On September 12, 2017, Uziewe opened a Brand Banking and Trust account ending in 6925. He opened the account in Global Investment's name and closed it on March 7, 2018. Between September 12, 2017, and March 7, 2018, there were a total of 166 credits to the account and 297 debits from the account. The credits and debits each totaled $864,633.

a. Significant credits include:

i. Wire transfers totaling approximately $288,950 from seven purported companies in the business of international logistics, global exports, and real estate.

ii. An approximately $29,620 wire transfer from a female in Toronto, Canada.

b. Significant debits include:

i. A total of approximately $242,643 in checks and transfers Uziewe wrote or sent to himself.

ii. A total of approximately $84,342 in cash withdrawals.

iii. A total of approximately $446,442 sent to purported international companies and individuals with references to shipping manufactured goods, logistical services, and real estate development.

iv. An approximately $62,000 wire transfer to Ovuomarhoni Naomi Isioro in Lagos, Nigeria.

83. On September 15, 2017, Uziewe opened a United Community Bank account ending in 9218. He opened the account in Global Investment's name and closed it on October 2, 2017. Between September 15, 2017, and October 2, 2017, there were a total of 3 credits to the account and 16 debits from the account. The credits and debits each totaled approximately $78,567.

a. Significant credits include an approximately $49,650 check from a 59 year old woman from Brooklyn, New York.

b. Significant debits include:

i. Two checks totaling approximately $28,000 that Uziewe wrote to himself that reference vehicle purchases.

ii. An approximately $19,270 counter withdrawal.

84. On October 10, 2017, Uziewe opened a Woodforest National Bank account ending in 3387. He opened the account in Didimiki's name and closed it on January 23, 2018. Between October 10, 2017, and January 23, 2018, there were a total of eight credits to the account and 31 debits from the account. The credits and debits each totaled approximately $107,012.

a. Significant credits include two wire transfers totaling approximately $86,500 from Bank of America accounts held by an unknown person or organization that reference "Services."

b. Significant debits include approximately $57,565 in cash withdrawals.

85. On March 2, 2018, Uziewe opened a SunTrust Bank account ending in 4026. He opened the account in Didimiki's name and closed it on June 11, 2018. Between March 2, 2018, and June 11, 2018, there were a total of 24 credits to the account and 47 debits from the account. The credits and debits each totaled approximately $167,057.

a. Significant credits include:

i. Approximately $92,009 in cash deposits.

ii. An approximately $47,000 wire transfer from "Brooks Harrison – Attorneys at Law."

b. Significant debits include: Approximately $72,975 in cash withdrawals.

86. On August 6, 2018, Uziewe opened a Synovus Bank account ending in 3410. He opened the account in Global Investment's name and closed it on November 30, 2018. Between August 6, 2018, and November 30, 2018, there were a total of 12 credits to the account and 107 debits from the account. The credits and debits each totaled approximately $742,199.

a. Significant credits include:

i. The approximately $205,000 cashier's check from romance scam victim K.P. referenced above.

ii. An approximately $160,000 cashier's check from an unknown individual from Livermore, California.

iii. The approximately $100,000 cashier's check from romance scam victim P.B. referenced above.

iv. The two cashier's checks totaling approximately $64,050 from romance scam victim M.B.B referenced above.

v. The approximately $36,249 cashier's check from romance scam victim M.E. referenced above.

vi. An approximately $97,400 cashier's check from V.G., a 71 year old woman from Woodbury, Minnesota.

vii. An approximately $27,000 cashier's check from a law firm.

viii. An approximately $15,000 wire transfer from a 69 year old woman from Bremerton, Washington, that references a General Joe Faulkner.

b. Significant debits include:

i. Twenty six checks totaling approximately $384,330 that Uziewe wrote to himself. The checks reference in the memo lines vehicle purchases, equipment purchases, housing expenses, inventory purchases, office expenses, office building renovations, office rent, office supplies, and real estate purchases.

ii. An approximately $104,346 check written to a purported company called Corner Global Medical Equipment Procurement LLC.

iii. An approximately $75,000 check written to Ogaga Onayomake.

iv. An approximately $100,000 wire transfer to an industrial truck dealer located in Mississippi as partial payment for the purchase of three 2018 Ford F-450 trucks. In October 2018, the three F-450 trucks were purchased in the name of Strategic Thrust LTD, a purported company located in Rhode Island, and shipped via Atlantic Container Lines from a port in Galveston, Texas, to Tin Can Island in

Nigeria.

v. Approximately $8,175 in debit card purchases at various restaurants and retailers.

87. On November 26, 2018, Uziewe opened an Entegra Bank account ending in 2175. He opened the account in Didimiki's name and closed it on January 14, 2019. Between November 26, 2018, and January 14, 2019, there were a total of 19 credits to the account and 44 debits from the account. The credits and debits each totaled approximately $381,964.

a. Significant credits include:

i. Approximately $260,505 in wire transfers from unknown individuals.

ii. Approximately $48,965 in cash deposits.

iii. A $30,000 cashier's check from V.G., the 71 year old woman in Woodbury, Minnesota, referenced above, payable to Didimiki Global Enterprises Corp.

b. Significant debits include:

i. Cash withdrawals totaling approximately $20,757.

ii. Debit card transactions at retail establishments totaling approximately $5,339.

iii. Two checks totaling approximately $58,600 that Uziewe used to withdraw cash. The checks reference vehicle purchases and office rental expenses in their respective memo lines.

iv. Four checks totaling approximately $50,480 that Uziewe wrote to himself. The checks reference in their memo lines real estate expenses, office expenses, bonus payments, and office furniture.

v. A single check totaling approximately $40,000 to Obafemi Martins. The check references manufactured goods for Didimiki.

vi. A total of approximately $206,394 comprised of four wire transfers to unknown beneficiaries and one counter withdrawal for an unknown beneficiary.

88. On November 26, 2018, Uziewe opened a South State Bank account ending in 6302. He opened the account in Global Investment's name and closed it on February 19, 2019. Between November 26, 2018, and February 19, 2019, there were a total of 13 credits to the account and 65 debits from the account. The credits and debits each totaled approximately $345,780.

a. Significant credits include:

i. A wire transfer and a cashier's check totaling approximately $106,000 from V.G., the 71 year old woman from Woodbury, Minnesota, referenced above.

ii. Approximately $45,880 in cash deposits,

iii. An approximately $64,000 wire transfer from E.S., a 76 year old woman from Studio City, California.

iv. An approximately $15,000 wire transfer from an unknown company.

b. Significant debits include:

i. Approximately $68,930 in cash withdrawals using personal checks that reference house rental repair, house renovation, building workers payment, movies expense, and vehicle purchase.

ii. Five separate checks totaling approximately $55,400 that Uziewe wrote to himself that reference relocation expenses, rental expense, office furniture, and office expense.

iii. Approximately $65,000 in checks written to an individual named Obafemi Martins that reference advance for property, land development, and advance for hospital bills.

iv. Approximately $8,008 in debit card purchases at various retailers.

2. Durojaye

89. On July 11, 2017, Durojaye opened a Wells Fargo account ending in 5415. He opened the account in Deuteronomy's name and closed it on November 9, 2017. Between July 11, 2017, and November 9, 2017, there were a total of 44 credits to the account and 71 debits from the account. The credits and debits each totaled approximately $577,391.

a. Significant credits include:

i. The approximately $204,845 cashier's check from romance scam victim P.P. that was comprised of funds from the BEC scheme targeting Victim Company 1.

ii. Approximately $136,140 in cash deposits.

iii. An approximately $26,000 wire transfer from a purported company called Granville

Procurement LTD LLC.

iv. An approximately $20,000 check from a 28 year old woman from South Lake Tahoe, California.

b. Significant debits include:

i. Fifteen wire transfers totaling approximately $378,102 to an unknown account in the name of Deuteronomy Integrated Services. Durojaye sent the majority of the funds to accounts at First City Monument Bank in Lagos, Nigeria, by wire transfers through a Citibank intermediary account.

ii. Approximately $110,360 in cash withdrawals.

90. On July 12, 2017, Durojaye opened a Bank of America account ending in 3024. He opened the account in Deuteronomy's name and closed it on August 4, 2017. Between July 12, 2017, and August 4, 2017, there were a total of eight credits to the account and 12 debits from the account. The credits and debits each totaled approximately $66,850.

a. Significant credits include:

i. Two wire transfers totaling approximately $37,000 from other Durojaye-controlled accounts.

ii. Approximately $29,750 in cash and check deposits.

b. Significant debits include three wire transfers totaling approximately $53,357 to Deuteronomy Integrated Services via a Citibank intermediary account. The destination accounts of the funds are unknown.

91. On August 9, 2017, Durojaye and his wife, Olabimpe Durojaye, opened a Wells Fargo account ending in 8430. The Durojayes closed the account on September 29, 2017. Between August 9, 2017, and September 29, 2017, there were a total of 11 credits to the account and eight debits from the account. The credits and debits each totaled approximately $55,225.

a. Significant credits include:

i. Approximately $36,200 in cash deposits.

ii. Two wire transfers totaling approximately $19,000 from a purported company called Mission Financial LTD.

b. Significant debits include:

i. A bank initiated account closing transaction of $38,904 indicated as a "loss prevention."

ii. An approximately $14,200 wire transfer to the purported company called Granville Procurement LTD LLC referenced above.

3. Wadur

92. On February 12, 2016, Wadur opened a JP Morgan Chase Bank account ending in 8917. He opened the account in Hasmaya's name and closed it on October 31, 2018. Between February 12, 2016, and October 31, 2018, there were a total of 65 credits to the account and 271 debits from the account. The credits and debits each totaled approximately $53,707.

a. Significant credits include:

i. Two deposits from unknown females totaling approximately $11,000.

ii. Approximately $8,970 in cash deposits.

b. Significant debits include:

i. Approximately $27,190 in cash withdrawals.

ii. Approximately $7,625 in retail purchases.

93. On June 2, 2017, Wadur opened a JP Morgan Chase Bank account ending in 6966. He opened the account in Hasmaya's name and closed it on August 14, 2017. Between June 2, 2017, and August 14, 2017, there were a total of seven credits to the account and 14 debits from the account. The credits and debits each totaled approximately $166,800.

a. Significant credits include:

i. The approximately $55,000 wire transfer from romance scam victim K.J.

ii. An approximately $50,000 check from a woman in Naples, Florida.

iii. An approximately $50,000 check from a man in Charlotte, North Carolina.

b. Significant debits include:

i. Approximately $119,238 in cashier's checks to Copart, an online auto auction.

ii. Approximately $8,600 in transfers to other Wadur-controlled accounts.

94. On June 28, 2017, Wadur opened a PNC Bank account ending in 6556. He opened the

account in Hasmaya's name and closed it on August 25, 2017. Between June 8, 2017, and August 25, 2017, there were four credits and 24 debits. The credits and debits each totaled approximately $315,840.

a. Significant credits include:

i. The approximately $302,290 cashier's check from romance scam victim P.P. that was comprised of funds from the BEC scheme targeting Victim Company 1.

ii. An approximately $9,000 check from a PhD in Denver, Colorado.

b. Significant debits include;

i. Seven cashier's checks totaling approximately $111,349 to Copart, an online auto auction.

ii. Three wire transfers totaling approximately $89,500 to a purported company called Dunkuul, Inc.

iii. An approximately $25,000 wire transfer to a medical center in Florida.

iv. Two wire transfers totaling approximately $45,000 to law firms.

v. An approximately $8,000 check to Insurance Auto Auctions, an online auto auction.

vi. Approximately $28,245 in cash withdrawals.

95. On August 3, 2017, Wadur opened a Keybank account ending in 8802. He opened the account in Hasmaya's name and closed it on December 11, 2017. Between August 3, 2017, and December 11, 2017, there were a total of 16 credits to the account and 37 debits from the account. The credits and debits each totaled approximately $336,937.

a. Significant credits include:

i. An approximately $84,380 deposit from a purported company called LAD Holdings LLP.

ii. Approximately $60,000 in wire transfers from a woman in San Francisco, California.

iii. An approximately $40,000 wire transfer from a 77 year old woman from Huron, Ohio.

iv. Two wire transfers totaling approximately $20,000 from a purported company called The Center for Better Health Inc DBA Southland Spine Rehab.

b. Significant debits include:

i. Approximately $193,641 in counter withdrawals.

ii. Approximately $32,198 in wire transfers and cashier's checks issued to Copart, an online auto auction.

iii. An approximately $23,000 wire transfer to a purported company called Dunkuul, Inc., in Rockford, Illinois.

96. On October 25, 2017, Wadur opened a Keybank account ending in 8836. He opened the account in Hasmaya's name and closed it on December 5, 2017. Between October 25, 2017, and December 5, 2017, there were two credits to the account and four debits from the account. The credits and debits each totaled approximately $45,053. A significant debit was an approximately $1,500 payment to Atlantic Container Line, which is the company referenced above that shipped the F-450 Ford trucks for which Uziewe provided partial payment to the truck dealer located in Mississippi.

F. Use of Electronic devices

97. Based on the investigation to date, I know the conspirators used electronic devices to carry out the scheme. As described above, the conspirators defrauded all of the identified romance scam victims using online communications. For example, romance scam victim P.P. met an individual purportedly named David Willson through an online dating website. She subsequently communicated with Willson using email and, later, through text and voice communications using an encrypted messaging application called Viber. These communications resulted in P.P. opening the account into which funds meant for Victim Company 1 were deposited and disbursing funds through cashier's checks to Global Investment (Uziewe), Hasmaya (Wadur), and Deuteronomy (Durojaye).

98. As another example, romance scam victim M.E. met an individual purportedly named Vinksey Walker through an online dating website. M.E. subsequently communicated with Walker through Facebook Messenger and, later, a Google Hangouts account associated with the email account westpointus2207@gmail.com. Those communications resulted in M.E. sending approximately $100,000 in checks to Global Investment.

99. Additionally, romance scam victim K.J. was defrauded by someone she met through the online dating website Match.com. Communications with that person resulted in K.J. wiring

approximately $55,000 to a Wadur-controlled account in Hasmaya's name.

100. Based on the purported Vinksey Walker's use of the westpointus2207@gmail.com to defraud M.E., federal agents served several search warrants on Google LLC for content and records for over 30 "westpointus" variant email addresses and accounts. The content and records revealed that the user or users of westpointus2207@gmail.com and users of other "westpointus" Google accounts used Google Hangouts to identify, recruit, and communicate with over 100 romance scam victims and targets, in addition to M.E. The conspirators also used Google Hangouts to communicate with each other to, among other things, discuss various romance scam victims and targets, to share different romance scam pickup lines and methods to develop relationships with potential romance scam victims, and to coordinate the destination of funds obtained from romance scam victims.

101. Through the Google Hangouts chat logs, law enforcement identified the user of westpointus55@gmail.com as high-up actor in the scheme who appears to direct the behavior of other conspirators. The user of wespointus2207@gmail.com and users of other "westpointus" Google accounts often refer to the user of westpointus55@gmail.com as the "chairman." And, at least in one chat log, the "chairman" appears to instruct an associate to direct money to Uziewe:

westpointus55@gmail.com: For that 5k

westpointus55@gmail.com: We still done use this one too

westpointus55@gmail.com: Bank Name : Michael UZIEWE Receiver Home address : 1911 Grayson Hwy , Suite 8-339Grayson GA 30017

102. In addition to the above, based on my training and experience and consultations with other law enforcement personnel, I know the following to be true about electronic devices, including wireless telephones and computers, being instrumentalities of BEC schemes and related romance schemes and containing evidence of those schemes:

a. Individuals involved in BEC and romance schemes use electronic devices, including wireless telephones and computers, to communicate with victims and one another by, among other things, voice and text messages, chat functions, and email. Electronic devices can preserve in their memory a history of incoming, outgoing, and missed calls and incoming and outgoing email, text messages, and chats, which can lead to

evidence of the telephone numbers, email addresses, and chat identifiers of others involved in the schemes and the dates and times they and/or the electronic device user communicated by telephone, text messages, chats, and email. Electronic devices also can contain in their memory contact information. This allows the user to store email addresses, phone numbers, and other contact information. The information stored in an electronic device used by individuals engaged BEC and romance schemes can identify victims and associations of the user, some of which are related to his or her illegal conduct.

b. Wireless telephones and computers also contain in their memory text messages and email communications sent, received, and drafted by the wireless telephone user. The communication history of individuals involved BEC and romance schemes may contain evidence of the schemes because it shows the communications or planned communications with victims and others involved in the schemes. Wireless telephones also have a voicemail function that allows callers to leave messages for each other. These messages can contain evidence both of a schemer's association with his or her conspirators and their joint criminal activity. Wireless telephones and computers also can contain other user-entered data files such as "to-do" lists. Wireless telephones and computers also can contain photographic and video files, which can be evidence of criminal activity when the user takes and stores pictures and videos of evidence of a crime.

c. Individuals involved in BEC and romance schemes often use electronic devices and their email, text messaging, chat, and voicemail functions to conduct their business. Such individuals often rely on these functions to communicate about, among other things, personal identification information, including credit card or financial account information, of victims; means and methods used to obtain such personal identification information; the use of such personal identification information to engage in the schemes; the disposition of proceeds obtained through the schemes; the

identities and locations of co-conspirators, victims, and others involved in or affected by the schemes; and efforts to avoid detection by law enforcement.

d. Individuals involved in BEC and romance schemes often maintain records tracking their activities. Records often remain for long periods of time to memorialize and track the status of past transactions. These records often are maintained as electronic or digital data on wireless telephones and computers.

III. TECHNICAL TERMS

103. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Electronic Device: All types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, wireless telephones, tablets, server computers, and network hardware.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by electronic devices on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some devices have static, i.e., long-term, IP addresses, while other computers have dynamic, i.e., frequently changed, IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Storage medium: A storage medium is any physical object upon which electronic data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving email, text messages, and chats, and participating in Internet social networks.

f. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

104. As described above and in Attachment B, the applications seek permission to search for records that might be found in the locations and on the persons to be searched, in whatever form they are found. One form in which the records might be found is data stored on an electronic device's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

105. *Probable cause.* I submit that, if an electronic device or storage medium is found in the locations and on the persons to be searched, there is probable cause to believe those records will be stored on that device or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media contain electronic evidence of how a device has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. It is, however, technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

106. *Forensic evidence.* As further described in Attachment B, these applications seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrants, but also forensic evidence that establishes how the electronic devices

were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence may be on the electronic devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers and communication programs can store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic device was in use. Electronic device file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within an electronic device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic device or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic device or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic device was remotely accessed, thus inculpating or exculpating the device owner. Further, electronic device and storage media activity can indicate how and

when the device or storage media was accessed or used. For example, electronic devices typically contain information that log user account session times and durations, activity associated with user accounts, electronic storage media that connected with the device, and the IP addresses through which the device accessed networks and the Internet. Such information allows investigators to understand the chronological context of device or electronic storage media access, use, and events relating to the crimes under investigation. Additionally, some information stored within an electronic device or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a device may show both a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the device user. Lastly, information stored within an electronic device may provide relevant insight into the device user's state of mind as it relates to the offenses under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that merely can be reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that, when an individual uses an electronic device, the individual's device generally will serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device also is likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used, data that was sent or received, and other records that indicate the nature of the offense.

107. *Necessity of seizing or copying entire electronic devices or storage media.* In most cases, a thorough search of information that might be stored on electronic devices often requires the seizure of the physical storage media and later off-site review consistent with the warrants. It sometimes is possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage

media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that easily can be viewed on site. Analyzing evidence of how an electronic device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Electronic devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. Taking the storage media off-site and reviewing it in a controlled environment, however, will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under the warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

108. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

CONCLUSION

109. I submit that this affidavit supports probable cause to search the Subject Location, as further described in Attachment A1, and Wadur, as further described in Attachment A2, including any wireless telephone he possesses, owns, maintains, or operates, and seize the items described in Attachment B.

REQUEST FOR SEALING

110. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets and subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets and subjects an opportunity to flee, continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

SETH ERLINGER, Special Agent
Federal Bureau of Investigation

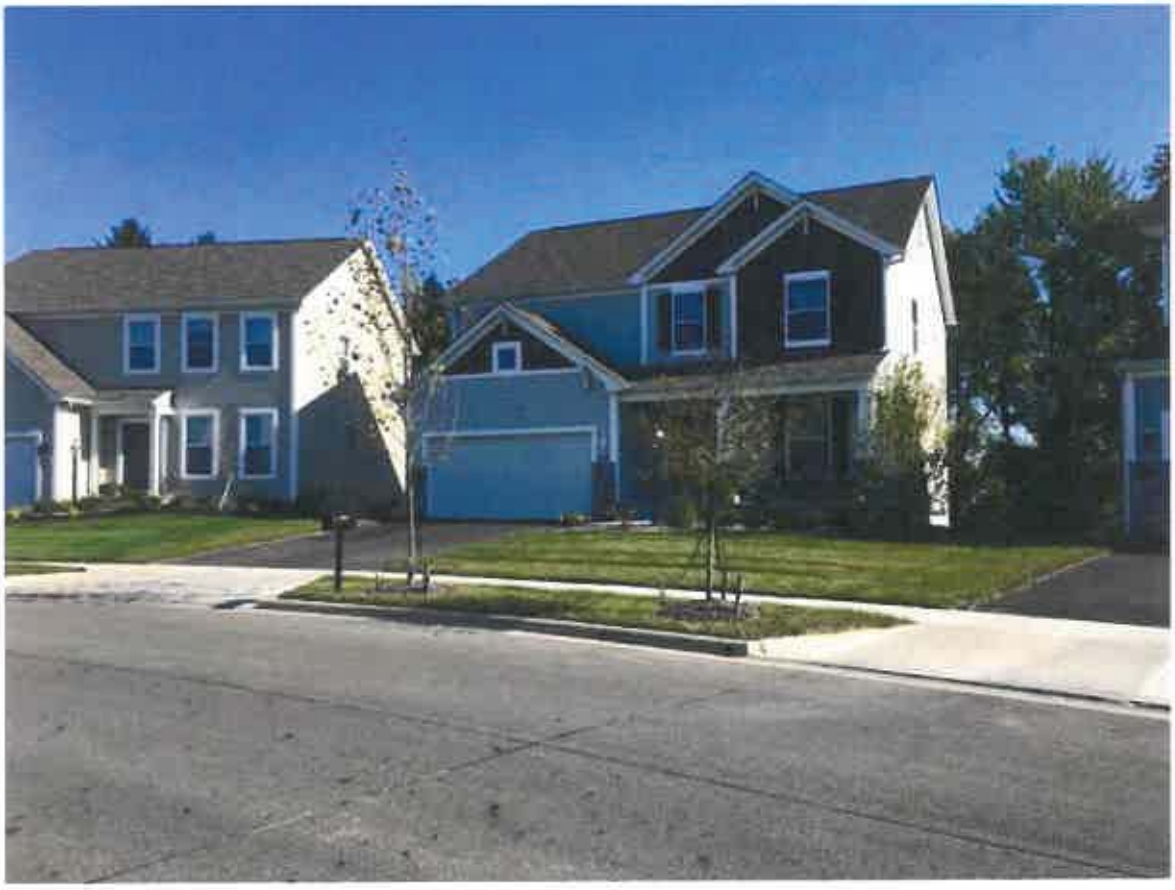
Subscribed and sworn to before me on:

The Honorable Chelsey M. Vascura
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1

Property to be searched

The location to be searched is located at 3252 Yellow Finch Way, Columbus, Ohio 43231 (located within the incorporated district of Minerva Park) ("Subject Location"). The Subject Location is further described as a grey, two-story single-family residential structure with white trim, and a black front door. A photograph of the Subject Location is below.



This warrant authorizes the search of all rooms, attics, basements, and all other parts within the Subject Location, whether locked or unlocked, and surrounding grounds, garages, and outbuildings of any kind, whether attached or unattached, locked or unlocked.

This warrant also authorizes the forensic examination of electronic devices at the location to identify the electronically stored information described in Attachment B.

ATTACHMENT A2 – Suleman Wadur

Person to be searched

The person to be searched is Suleman Wadur, as further described as a male with a birthdate of April 8, 1984, black hair, brown eyes, and an approximate height of 5'10" and weight of 150 pounds, including any wireless telephone or other electronic device he possesses, owns, maintains, or operates ("Subject Electronic Device").

This warrant authorizes the search of any and all clothing and personal belongings, including backpacks, wallets, briefcases, and bags within Suelman Wadur's immediate vicinity and control at the location where the search warrant is executed to locate the Subject Electronic Device. It shall not include a body cavity or strip search.

This warrant also authorizes the forensic examination of the Subject Electronic Device to identify the electronically stored information described in Attachment B.

ATTACHMENT B

Particular things to be seized

1. All records and information that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1028 (identify theft), 1028A (aggravated identity theft), 1030 (computer hacking), 1343 (wire fraud), 1344 (bank fraud), 1349 (conspiracy to commit wire and bank fraud), 371 (conspiracy), 1956 (money laundering and conspiracy to engage in money laundering), and 1957 (transactions in criminally derived property) (collectively, "Subject Offenses") involving

- Michael Oghale Uziewe, a.k.a. Michael Uziewe Oghale ("Uziewe"),
- Omodotun Titus Durojaye, a.k.a Titus Omodotun Durojaye ("Durojaye"),
- Suleman Wadur, a.k.a Suleman Bulama Wadur ("Wadur"),
- Global Investment Network Inc. ("Global Investment"),
- Hasmaya Group LLC, f.k.a. Hasmaya Energy Group Ltd. ("Hasmaya"),
- Deuteronomy Procurement Services, LLC ("Deuteronomy"),
- Didimiki Global Enterprises ("Didimiki"), and
- Eds Lead LLC ("Eds"),

(Global Investment, Hasmaya, Deuteronomy, Didimiki, and Eds, collectively, "Subject Companies"), including records and information relating to:

a. Business email compromise schemes, romance schemes, and other related fraudulent schemes;

b. Acquisition and use of stolen and fraudulent identities;

c. Creation and use of email and other online accounts;

d. Compromise and spoofing of email accounts;

e. Unauthorized access of computer systems;

f. Selection and targeting of victims;

g. Wire transfers, checks, money orders, money service payments, and other financial transactions, as well as solicitation of such transactions;

h. Financial accounts, checks, credit cards, debit cards, electronic benefit cards, and other financial instruments;

i. Tax documents, including federal and state income tax returns, W-2s, 1099s, and other documents showing income;

j. Laundering proceeds of the Subject Offenses;

k. Formation, ownership, and control the Subject Companies and any related companies;

l. Location, storage, and concealment of cash, money instruments, and money equivalents;

m. Currency, commercial paper, financial instruments, and other forms of stored value in excess of $5,000;

n. Preparatory steps taken in furtherance of the Subject Offenses;

o. Communications in any form related to the Subject Offenses;

p. Contacts and related identifying information;

q. Address books, appointment books, calendars, and schedules;

r. Pictures and videos;

s. Domestic and international travel records;

t. Identities, locations, and contact information of co-conspirators, victims, and others involved in or affected by any of the Subject Offenses;

u. Efforts to avoid detection by law enforcement; and

v. Contextual information necessary to understand the evidence described in this attachment.

2. Electronic devices, including wireless telephones, computers, tablets, and storage media used as a means to commit the Subject Offenses.

3. For any wireless telephone, computer, tablet, and storage medium whose seizure is otherwise authorized by this warrant, and any wireless telephone, computer, tablet, and storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("electronic device"):

a. evidence of who used, owned, and controlled the electronic device at the time the things described in this warrant were created, edited, and deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the electronic device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence and absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the electronic device was accessed and used to determine the chronological context of electronic device access, use, and events relating to the Subject Offenses and to the electronic user;

e. evidence indicating the electronic user's state of mind as it relates to the Subject Offenses;

f. evidence of the attachment to the electronic device of other storage devices and similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic device;

h. evidence of the times the electronic device was used;

i. incoming, outgoing, and saved communications, including telephone calls, text messages, chats, and emails, including the contents of communications;

j. passwords, encryption keys, and other access devices that may be necessary to access the electronic device;

k. documentation and manuals that may be necessary to access the electronic device and to conduct a forensic examination of the electronic device;

l. applications, utility programs, compilers, interpreters, and other software that may be necessary to access the device.

m. records of and information about Internet Protocol addresses used by the electronic device;

n. routers, modems, and network equipment used to connect the electronic device to the Internet;

o. records of and information about the electronic device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" and "favorite" web pages, search terms the user entered into any Internet search engine, and records of user-typed web addresses;

p. address books, appointment books, "to-do" lists, calendars, and schedules; and

q. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may be created or stored, including any form of electronic device or electronic storage (such as hard disks or other media that can store data), any handmade form (such as writing), any mechanical form (such as printing or typing), and any photographic or videographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, recordings, pictures, or photocopies), and includes communications in whatever form and however stored (including, but not limited to, text and instant messages, chats, emails, or telephone calls).

The term "electronic devices" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, wireless telephones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which electronic device data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.